Meeting Summary

eHealth Technical Working Group
January 20, 2010 11:00AM-12:30PM

Please refer to the draft straw man architecture document for additional information.

Co-Chairs and TAC Liaison:
After a call for volunteers and a selection process by CHHS, Scott Cebula and Rim Cothren have been appointed as co-chairs of the TWG. In addition, Rim will be serving as the liaison to TAC.

The role of the co-chairs will be to work with the staff in helping to guide the committee through its work to complete the technical design process. Co-chairs will draw the group's attention to relevant questions, reach out to other groups by expressing information needs and responding to information requests, and represent TWG in other forums as needed.

Review of Straw Man Architecture Draft:
Purpose, Description, and Operational Policies
Walter asked the group whether there were comments pertaining to the Purpose, Description, Operational Policies sections of the draft document. There being no comments, the group was asked whether there were any strong objections to anything in these sections. There was consensus that these sections represented the thinking of the group.

Tim Andrews suggested that the document should acknowledge the importance of two additional capabilities that need to be defined for the proper functioning of the Registry Service:

1. Who will perform provisioning and how electronic credentials will be managed over time
2. Who will provide enforcement of policies and how settlement of disputes will be handled

Registry Service and Trust Framework
At the last TWG meeting, it was decided that TAC would need to provide guidance with respect to whether the Authentication Service should support individual-level or system-level authentication. A discussion ensued regarding issues related to the trust framework and the handling of individuals within that framework.

One question that emerged was how and where to represent individuals within the system for the purposes of correct addressing. The following points were made by participants:

- Rim Cothren suggested that individuals would be represented in the registry in association with a system that is authenticated.
- Dave Handren stated that it would be unmanageable to have individuals in the registry. It was then suggested that the registry only have systems, while the routing service contain the addressing information of individuals.

- Walter pointed out that addressing necessitates proper identification. The role of the Registry Service is to provide a trusted binding of an identity to attributes such as physical address, specialty, and role such that individuals can be reliably distinguished from one another. Thus, it would seem that individuals would still need to be provisioned and credentialed so that their information exists in the registry, even if they were not going to be authenticated by the Authentication Service.
- Dave Handren stated that it may not be necessary to specify individual information in the system; rather, communication would be between organizations, with sender and recipient information sent in the message. In response to this, Tim Andrews brought up the point that identification of individuals within the system would nevertheless be necessary to be able to push data to the appropriate person.

Another issue raised had to do with the viability of the trust framework should individual-level authentication occur at the organizational level (as opposed to the CS-HIE Services level). The following main points were expressed:

- Dave Handren stated that trust between organizations could be sufficiently supported if a DURSA is in place between the data trading partners, the proper level of patient consent has been obtained, and there is a way for organizations to perform auditing at the transaction level (e.g., date/time, requestor, event, and payload).
- Rim Cothren added that organizations can define varying levels of patient consent for different data use purposes, which would allow organizations to approve or deny data requests depending on the role of the requestor and purpose of the request. Rim also explained that trust at the organizational level would involve certification of organizations in the registry. The certification process would require organizations to agree to authenticate individuals on their systems through their policies, and to take responsibility for assertions of individuals' identities and proper use of the data.
- Walter pointed out that according to feedback received from Orlando Portale last week, some large organizations may not trust that other organizations (particularly smaller ones) have properly authenticated their users. Tim Andrews concurred that this has been a problem that he has observed in the past, and that many large organizations will not agree to a DURSA because they demand visibility into the organizational processes and procedures of the counterparties.
- The practicality of creating bilateral data use agreements among the myriad of data trading partners in California is an issue. It is unclear whether there is a way to institute a common data use agreement that could be signed by all entities.
- Tim Andrews stated that based on his experience in two other states, Medicaid has insisted upon authenticating individual providers and will not accept trusted certificates from an intermediary. Thus, it would be critical to get the perspective of Medi-Cal in making a decision about how to proceed with the trust framework.
- Walter suggested that a middle ground between pure systems-level authentication and obligatory individual-level authentication would be to provision all participating entities

(whether enterprises or individuals) in the registry, but to leave the means of authenticating users against the credentialed entities in the registry up to the enterprises themselves as opposed to requiring authentication through a centralized authentication service. Dave Handren agreed that this could be an alternative.

In the end, the group agreed to table further discussion until TAC's input could be sought.

Technical Aspects of Registry Service

Walter asked whether UDDI would support the registry functions and specifications as described in the draft document, and whether NHIN's use of UDDI for the NHIE Service Registry represents the appropriate framework for what is needed in California. (Currently, NHIN is using UDDI to register HIOs, although in the future, the registry may be regionalized by state and possibly by county.) Based on the knowledge of group members, UDDI should be able to support the required functions of the registry. However, it is unknown whether UDDI will efficiently handle a registry with the number of registry entries (potentially hundreds of thousands of enterprises and/or individuals) required by CS-HIE Services. Of note, the UDDI specification does support federation of registries so that instead of a single registry there can instead be multiple regional registries that together hold all CS-HIE participants.

LDAP, which is being used by the caBIG community. was mentioned as a potential alternative to UDDI. Additional information is needed to assess suitability for the present purpose.

In general, the group believed that the registry did not pose an architectural problem, and felt confident that a solution could be found to achieve acceptable performance.

Routing Service

Walter asked for feedback on the technology description of the Routing Service as utilizing the UDDI model.

- Rim Cothren, who had provided written comments earlier, clarified that his expressed concern about UDDI being potentially inappropriate for the purpose needed to be validated because it was based on second-hand knowledge and was largely a concern about performance issues.
- Tim Andrews pointed out that the UDDI tModel object has the capacity for multiple bindings, which would provide a way to specify multiple protocols for a given transaction type.
- The performance characteristics of UDDI are unknown in the setting of a large implementation such as the one proposed.
- LDAP would be an alternative to UDDI, although performance is once again unknown.
- Walter asked whether it made sense that the network address could be stored in the BindingTemplate, and the protocol suite stored in the tModel. Tim Andrews volunteered to find out the validity of this approach from contacts with expert knowledge of UDDI.

Authentication Service

The need for an Authentication Service as described in the draft document is dependent upon whether the trust framework will be based on individual-level or system-level authentication. A trust model of provisioned systems (as opposed to individuals) will require mutual authentication between systems using a secure transport protocol (e.g., TLS) leading to the establishment of long-lived connections between trusted systems, creating a network backbone. Further discussion about the Authentication Service was tabled until additional guidance from TAC is obtained.

Next Steps:

- Walter and Rim will ask TAC to provide input regarding whether it is necessary to support centralized individual-level authentication as part of the trust framework.
- Next meeting will be the week of 2/1.

Summary of Key Questions/Issues/Decision Points:

- Is centralized individual-level authentication needed to establish trust for CS-HIE services?
- Does a registry that provisions all participating entities (both enterprises and individuals) establish a desirable "middle ground" trust solution between required, centralized individual-level authentication and only authenticating systems?
- UDDI and LDAP specifications appear to support the desired functionality of the Registry Service and Routing Service. However, there are unanswered questions about how such technologies will perform in the large-scale setting required by the current purpose of HIE in California.
- Is an Authentication Service necessary if the trust framework is based on system-level trust?

Members Present

Name	Organization
Jane Brown	Nautilus Healthcare Management Group
Scott Cebula	Independent
Paul Collins	CA Dept. of Public Health
Robert("Rim") Cothren	Cognosante, Inc.
Dave Handren	Long Beach Network for Health
Daniel Haun	Adventist
Jen Herda	Long Beach Network for Health
Kathryn Lowell	CA Business, Transportation and Housing Agency
Lee Mosbrucker	CA Office of the Chief Information Officer
Jim Thornton	MemorialCare
Ben Word	CA Dept. of Health Care Services
Kris Young	CA Office of Health Information Integrity

Staff Present

Name
Walter Sujansky
Tim Andrews
Peter Hung